REMARKS

Applicant appreciates the Office's consideration of pre-appeal comments submitted on August 18, 2005. Applicant respectfully requests reconsideration and allowance of the subject application. Claims 1-30 are pending in the application. Claims 1, 13, 19, 24, 27 and 30 are independent claims.

Interview

The Applicant appreciates the time afforded to the Applicant's representative during a telephone interview of December 14, 2005. During the interview, the Examiner and the Applicant's representative discussed in detail the Spies et al. patent. An agreement was not reached during the interview.

Overview

The primary patent relied upon by the Office, Spies et al., teaches an arrangement for providing video content to merchants. This video content is delivered to the merchants in a state that cannot be played on a replay device. Separately, keys to enable the video content are delivered to the merchants. The keys may be delivered by way of a network, or via a floppy disk. The keys are not associated with the video content that they enable; the video content is kept on one storage location, and the keys are stored elsewhere.

Claim 13 of the subject application recites "content on [a] removable storage medium," "obtaining the one or more keys from the removable storage medium,... wherein the one or more keys are for decrypting content on the removable storage medium" and "communicating the one or more keys to the remote client computing device." Thus, the keys communicated to the client are

obtained from the removable storage medium that also contains the content. Spies et al. do not teach the foregoing. The claim further recites that "the one or more keys from the DVD [are] also usable to verify authenticity of the DVD drive." There is nothing in the Spies et al. patent that teaches this concept either. Further discussion of the claims and the rejections asserted in the current Office Action is provided below.

Claim Rejection Under 35 U.S.C. §§ 102 & 103

Claims 13, 17-18, 19-21, 23-25 and 27-28 stand rejected as being anticipated under §102 in view of US Patent 6,055,314 to Spies et. al (hereinafter "Spies"). Claims 1, 3, 4 and 6-11 stand rejected as being unpatentable under §103 over Spies in view of U.S. Patent 6,272,283 to Nguyen. Claims 2, 12, 14, 15, 16, 26 and 29 stand rejected as being unpatentable under §103 over Spies and Nguyen, and further in view of Powerfile C20 FAQs (hereinafter "Powerfile"). Finally, claims 5 and 22 stand rejected under §103 over Spies in view of a description of DirectShow (www.compressionworks.com). These rejections are respectfully traversed.

Spies discloses a system in which a customer, when purchasing a DVD or otherwise purchasing video content, also receives "decryption capabilities" from the vendor of the DVD. In the case of purchasing a DVD, the decryption capabilities are placed on an IC card that is carried by the user. In one described scenario, the user presents the IC card to the vendor when purchasing the DVD, and the vendor transfers the decryption capabilities to the IC card. (*Column 6, lines 11-33.*) The decryption capabilities can include a "program key." In another scenario, the decryption capabilities can be obtained via network and then stored

on the IC card. (*Column 6, lines 34-58.*) Once the decryption capabilities are in the IC card, the IC card is used in conjunction with a playback device to decrypt the purchased DVD or other video content.

Before the above can occur, according to Spies, a video merchant performs an initial transaction with a video content provider. The video content provider maintains a video program storage 30 and a program keys database 32. The video program storage 30 has a plurality of video content programs that the video merchant might want to sell. The program keys database 32 includes a number of program keys that enable use of the video content programs stored in the program storage 30. (*Column 5, lines 10-18.*) The video merchant contacts the video content provider to obtain video content and keys that will enable use of the obtained video content.

The process of obtaining video content and associated keys is summarized in the following. In one example, the video merchant obtains video content that is for resale. At this point, the video content cannot be played/consumed. The video content may be sent to the video merchant over a distribution network, or may be delivered to the merchant on portable media, such as digital video disks. (*Column 5, lines 25-32.*) The video content, whether delivered via network or by way of portable media, is not sent with enabling playback keys that may be used to enable playback of the video content.

The video merchant is now ready to accept keys that will enable video content that the merchant is authorized to sell. (*Column 5, lines 36-39.*) Spies gives several examples as to how these keys can be conveyed to the video merchant. One way is over a secure or insecure link, where the keys are conveyed in encrypted form. (*Column 5, lines 40-43.*) Spies also mentions that the keys

may be "ported on a floppy disk" to the merchant (*Column 5, lines 43-44.*) The Office is earnestly requested to keep the foregoing sentence in mind when considering the remainder of this Response. The reasoning being that Spies is porting *only* keys on floppy disk, not keys *and* the video content that the keys enable.

The Spies et al. patent is also silent regarding the additional subject matter added to claims 1, 13 and 19.

It is respectfully submitted that the mechanisms described by Spies do not include the elements recited by the claims.

Independent claim 13 recites "content on [a] removable storage medium," "obtaining the one or more keys from the removable storage medium,... wherein the one or more keys are for decrypting content on the removable storage medium and for verifying authenticity of the DVD drive" and "communicating the one or more keys to the remote client computing device." Thus, the keys communicated to the client are obtained from the removable storage medium that also contains the content.

Spies does not disclose this. The Office maintains the Spies disclosure found at column 5, lines 35-45, column 6, lines 34-58, column 13, lines 24-30, column 4, lines 35-53, column 12, lines 25-30, and column 9, lines 9-11 teaches the limitations indicated from claim 13. The Applicant disputes this conclusion for the following reasons.

Column 5, lines 35-45, teaches that keys are delivered to a video merchant to enable use of video content. As discussed above, this is done over a network or via disk. However, the delivery of the keys does not include delivery of the video content that the keys enable. To do this would defeat the purpose of the Spies

system; Spies wants to keep the keys and the video content separate to protect against unauthorized interception of video content. (*Column 16, lines 55-67.*) Therefore, this section of Spies does not teach or suggest at least "obtaining the one or more keys from the removable storage medium,... wherein the one or more keys are for decrypting content on the removable storage medium."

Column 6, lines 34-58, teaches how a user can go about purchasing video content from a video merchant and enabling the purchased video content for playback. In this example, the user selects and receives the video content over a network. However, the video content is not received in a format that is enabled for viewing. The user receives a key that enables viewing of the video content separately. The key is not sent with the video content, nor is the key associated with the video content. As was discussed earlier, the video content and the keys are kept separately. The video content is stored on a storage 30, and the keys are stored in a database 32. Therefore, this section of Spies does not teach or suggest at least "obtaining the one or more keys from the removable storage medium,... wherein the one or more keys are for decrypting content on the removable storage medium."

Column 13, lines 24-30, teaches particulars of a video purchasing application 168 that may be used to purchase video content available for purchase from the video merchant. Nothing in this section of Spies even remotely approaches the indicated limitations of claim 13.

Column 4, lines 35-53, encompasses part of the Brief Description of the Drawings section and one paragraph of the detailed description. This section states, for context, that a reader of the Spies document is assumed to have

knowledge of basic cryptography. As with the other sections discussed above, nothing in this section teaches or suggests the indicated limitations of claim 13.

Column 12, lines 25-30, teaches that generated keys are intended for "sessional" use. This means that a key generated for a particular video content is not used for another particular video content. As a matter of fact, this section of Spies indicates that a key is destroyed after it is distributed to an authorized customer. This section makes no mention of where the keys are coming from. Moreover, the section does not reference a source of the video content. Therefore, there is nothing in this section that teaches or suggests "obtaining the one or more keys from the removable storage medium,... wherein the one or more keys are for decrypting content on the removable storage medium."

For the reasons discussed above, Spies fails to disclose every element of claim 13, and the §102 rejection of claim 13 is invalid. Allowance of claim 13 is respectfully requested.

Dependent claims 14-18 are allowable because of their dependence from allowable base claim 13, and also for their additionally recited elements. Although claims 14-16 are rejected as being obvious over a combination of Spies, Nguyen and Powerfile, Nguyen and Powerfile do not describe the elements discussed above that are absent from Spies. Therefore, the arguments above apply as well to claims 14-16; Powerfile and Nguyen are not asserted by the Office to suggest transferring keys from the storage medium itself.

Independent claim 19 recites "a key exchange process with a disc drive in order to decode media content on a disc accessible to the disc drive." In addition, claim 19 recites "communicating . . . one or more keys from the disc that can be used at the computing device to decode the particular media content, the one or

more keys form the disc also usable to verify authenticity of the disc drive." Spies does not disclose this subject matter. Again, the Office relies on the passages discussed above in connection with the rejection of claim 13. However, these passages of Spies do not mention, teach or suggest the concept of obtaining a key from "the disc that can be used at the computing device to decode the particular media content," where the disc originating the key also contains content that can be decoded with the key.

Allowance of claim 19 is therefore requested.

Dependent claims 20-23 are allowable because of their dependence from allowable base claim 19, and also for their additionally recited elements. Although claim 22 is rejected as being obvious over a combination of Spies and DirectShow, DirectShow does not describe the characteristics indicated above that are absent from Spies. Therefore, the arguments above apply as well to claim 22.

Independent claim 24 recites a server component, and a DVD drive on the server component. In addition, claim 24 recites that the server component "operates as an intermediary between a DVD player on the client component and a DVD drive on the server component." Again, Spies does not show this.

In addressing this element, the Office relies upon Spies at col. 12, lines 8-53. This portion of Spies describes various details relating to key exchange, and starting at line 39, describes how a viewer decrypts video from a distribution medium. The decryption involves the "viewer computing unit," the IC card, and a DVD reader. However, Spies does not describe a server component that has a DVD drive and that "operates as an intermediary between a DVD player on the client." The Office has not indicated any proposal for how the components of

Spies might be correlated to the elements recited in claim 24, and the Applicant does not believe any reasonable correlation exists.

Accordingly, it is believed that claim 24 is allowable.

Dependent claims 25-26 are allowable because of their dependence from allowable base claim 24, and also for their additionally recited elements. Although claim 26 is rejected as being obvious over a combination of Spies, Nguyen and Powerfile, Nguyen and Powerfile do not describe the characteristics indicated above that are absent from Spies. Therefore, the arguments above apply as well to claim 26; Nguyen and Powerfile are not asserted by the Office to suggest "an intermediary between a DVD player on the client component and a DVD drive on the server component."

Independent claim 27 recites a server component configured to "exchange Content Scrambling System (CSS) keys between a DVD drive of the system and the key exchange client component." Spies does not describe exchanging keys between a DVD drive and any other component.

In rejecting claim 27, the Office states that this element is addressed by Spies at col. 12, lines 8-53. Within these lines, however, Spies only discusses a DVD drive at lines 49-53. And within lines 49-53, Spies does not discuss exchanging keys with a DVD drive.

Accordingly, Spies does not show every element of claim 27, and should be allowed.

Dependent claims 28-29 are allowable because of their dependence from allowable base claim 27, and also for their additionally recited elements. Although claim 29 is rejected as being obvious over a combination of Spies, Nguyen and Powerfile, Nguyen and Powerfile do not describe the characteristics

indicated above that are absent from Spies. Therefore, the arguments above apply as well to claim 29; Nguyen and Powerfile are not asserted by the Office to suggest exchanging keys between a DVD drive . . .."

Independent claim 1 recites a server device having a "DVD drive," and a " key exchange server." A client device has "a key exchange client and a decoder". Claim 1 further recites that the "key exchange client and the key exchange server communicate with one another to pass one or more keys *from the DVD* to the key exchange client to allow the decoder to decrypt *content* received, via the network, *from the DVD*, the one or more keys from the DVD also usable to verify authenticity of the DVD drive." Spies does not disclose passing one or more keys from a DVD. Nor does Spies does teach or suggest the concept of decrypting content received over a network using a key, where the key and the content come from the same source (i.e., the DVD). Further more, Spies does not teach or suggest that the one or more keys from the DVD are also usable to verify authenticity of the DVD drive.

In addressing the element of claim 1, the Office references column 3, lines 40-45 of Spies. This paragraph states that a content provider supplies an encrypted video stream on a network or DVD. The last sentence of the paragraph states that decryption is performed at the client by using the decryption capabilities of the IC card. Lines 40-45 do not discuss keys other than the "stored program key" held by the IC card. There is no description of any keys being transferred "from the DVD" to a client.

In addressing the element of claim 1 further, the Office references column 6, lines 55-58. This portion of Spies is discussed in detail earlier in this Response. There is nothing in this portion of Spies that teaches or suggests passing "one or

more keys *from the DVD* to the key exchange client to allow the decoder to decrypt *content* received, via the network, *from the DVD*."

The Office admits that Spies fails to teach or suggest "passing the cryptographic keys from the DVD to the key exchange client," and relies upon Nguyen to make up for this deficiency. However, there is nothing in Nguyen that can remedy the Spies deficiency discussed in detail herein. In particular, the combination of Spies in view of Nguyen does not teach or suggest at least passing "one or more keys *from the DVD* to the key exchange client to allow the decoder to decrypt *content* received, via the network, *from the DVD*."

Accordingly, Spies fails to disclose every feature of claim 1, and the §103 rejection of claim 1 is unfounded. Withdrawal of the rejection is respectfully requested.

Dependent claims 2-12 are allowable because of their dependence from allowable base claim 1, and also for their additionally recited elements. Although claims 2 and 12 are rejected as being obvious over a combination of Spies, Nguyen and Powerfile, Nguyen and Powerfile do not describe the characteristics indicated above that are absent from Spies. Therefore, the arguments above apply as well to claims 2 and 12; Nguyen and Powerfile are not asserted by the Office to suggest transferring keys from the storage DVD. Although claim 5 is rejected is rejected as being obvious over a combination of Spies and DirectShow, DirectShow does not describe the characteristics indicated above that are absent from Spies. Therefore, the arguments above apply as well to claim 5.

Addition **independent claim 30** recites the subject matter "the key exchange client and the key exchange server communicate with one another keys from the DVD to the key exchange client, at least one of the keys to allow the

decoder to decrypt content received, via the network, from the DVD, and another of the keys is specific to a media content player incorporating the decoder, and wherein the server component obtains, based on information received from the client component, an appropriate key for the media content player." This subject matter is neither taught nor suggested by any of the documents relied upon by the Office. Therefore, it is respectfully submitted that this claim is in condition of allowance.

Conclusion

All claims are in condition for allowance. Applicant respectfully requests prompt allowance of the subject application. If any issue remains unresolved that would prevent allowance of this case, **the Examiner is requested to contact the undersigned attorney to resolve the issue**.

Respectfully Submitted,

Date: 12/16/05

By: Tim R. Wyckoff

Tim R. Wyckoff
Lee & Hayes, pllc
Reg. No. 46,175
(206) 315-4001 ext. 110